

Applying Gamification to Teaching Cyber Security

Reece Buckle

Supervisor: Nawfal Fadhel

October 23, 2020

Problem

Despite the existence of many cyber security awareness programs, there is still a lack of widespread cyber security training in a world where the number of people interacting with technology is ever increasing

As modern day technology is ever evolving, the number of users who interact with technology increases consequently. As a result, the risk of becoming a victim to cybercrime is ever increasing. In particular, small and medium-sized enterprises (SMEs) are the biggest sectors which are hit hardest by cybercrime (Bada, Maria & Nurse, 2019). This is mostly due to the fact that smaller businesses and employees struggle to understand the importance of cyber security and often cannot afford consistent cyber security training (Bada, Maria & Nurse, 2019).

Because most cyber attacks are successful due to social engineering and human error, many government schemes, compliance regulations and training material exist to tackle this problem. However, it has also been shown that game-based learning can have a strong impact on the learning outcomes of cyber security in comparison to similar tutorials or training material (Tioh, Mina & Jacobson, 2017). Therefore, this project will aim to address the problem of an individual falling victim to cybercrime by creating a serious game.

Goals

The main goal of this project is to investigate the practicality and effectiveness of gamification, and ‘serious games’, in order to teach good cyber security principles. To do this, I will aim to create an educational tool which is inspired by pre-existing research of successful gamification techniques; it is my hope that the user will remain engaged until the end of its length such that the game fulfills its purpose and the user is left better equipped at protecting themselves from cybercrime. Finally, the application will adhere to key HCI/UX principles in order to provide a good user experience for users of all abilities.

Scope

The cyber security game will be multi-platform such that it is accessible to people using phones, tablets or their desktop computer. It will also be important to research gamification techniques for learning as well as gamification applied to cyber security specifically. Lastly, this project will also delve into researching the most common cyber attacks and how to tackle them effectively for the purpose of training.

Learning Objectives

- To develop a solid understanding in web and/or mobile application development tools which will incorporate both front end and back end design
- To make the game with a sleek and easy to use interface which adhere to key teachings in HCI/UX
- To gain a stronger understanding in how gamification can be used to teach serious problems such as cyber security.
- To develop a stronger understanding about the most effective methods to mitigate cybercrime

References

- Bada, Maria & Nurse, Jason. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs).
- Tioh, Jin-Ning & Mina, Mani & Jacobson, Douglas. (2017). Cyber security training a survey of serious games in cyber security.